Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 3, 5-8, 11-14, 16-21, 46, 48-54 and 68-79 are pending in the application, with claims 68, 73, and 78 being the independent claims. Claims 15 and 55 are sought to be cancelled without prejudice to or disclaimer of the subject matter therein. Claims 5, 6, 11, 12, 46, 68, 71, 73, 76, and 78 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 112

Claims 11 and 12 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 11 and 12 were amended by the above amendment, rendering the rejection moot. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Rejections under 35 U.S.C. § 103

Schneier and Den Boer

Claims 3, 5-8, 11-12, 15, 17-21, 46, 48, 49, 51, 52, 55, and 68-79 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier, *Applied*

Cryptography (Schneier) in view of Den Boer, U.S. Patent Application No. 20020034295 (Den Boer). Applicants respectfully traverse this rejection.

In the Office Action, the Examiner stated that although Schneier explicitly fails to teach "an inverse permutation logic performing an inverse permutation of a bit sequence," this element is disclosed in Den Boer. In Den Boer, an input message block, M, is divided into a first part, M1, and a second part, M2. (Den Boer, ¶[0038]). The first part, M1, is processed using a non-linear function, g. (Den Boer, ¶[0038]). The second part, M2, is processed using an inverse function, g^{-1}. (Den Boer, ¶[0038]). Each of the functions, g and g^{-1}, merge M1 with key K1 and M2 with key K2, respectively. (Den Boer, ¶[0038]).

Independent claims 68, 73, and 78 were amended by the above amendment. The combination of Schneier and Den Boer does not teach or suggest each and every element of amended independent claims 68, 73, and 78. Specifically, the combination does not teach or suggest:

> a first inverse permutation logic for performing , during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;
>
> a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;
>
> means for combining via a second logical operation the third bit sequence with the second inverse permuted bit sequence to generate a fourth bit sequence; and
>
> a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

as recited in amended independent claims 68 and 73. In addition, the combination does not teach or suggest:

> a first inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the first portion of the data block and for generating a first inverse permuted bit sequence, wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;
> a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;
> a second XOR logic performing a second XOR operation of the third bit sequence and the second inverse permuted bit sequence to generate a fourth bit sequence; and
> a permutation logic for permuting the fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

as recited in amended independent claim 78. For at least these reasons, amended independent claims 68, 73, and 78 are patentable over the combination of Schneier and Den Boer. Claims 3, 5-8, 11, 12, 17-21, 69-72 depend from claim 68; claims 46, 48, 49, 51, 52, and 74-77 depend from claim 73; and claim 79 depends from claim 78. For at least these reasons and further in view of their own features, claims 3, 5-8, 11, 12, 17-21, 46, 48, 49, 51, 52, 69-72, 74-77, and 79 are patentable over the combination Schneier and Den Boer. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Schneier, Den Boer, and Steinman

Claims 13, 14, 53, and 54 were rejected under 35 U.S.C. §103(a) as being unpatenable over Schneier in view of Den Boer and further in view of Steinman, et al, U.S. Patent No. 6,591,349 (Steinman). Applicants respectfully traverse this rejection.

Claims 13 and 14 depend from amended independent claim 68 and claims 53 and 54 depend from amended independent claim 73. Steinman does not overcome the deficiencies of Schneier and Den Boer relative to claims 68 and 73, described above. For at least these reasons, and further in view of their own features, claims 13, 14, 53, and 54 are patentable over the combination Schneier, Den Boer, and Steinman. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Schneier, Den Boer, and Teppler

Claims 16 and 50 were rejected under 35 U.S.C. §103(a) as being unpatenable over Schneier in view of Den Boer and further in view of Teppler, et al, U.S. Patent No. 6,792,536 (Teppler). Applicants respectfully traverse this rejection.

Claims 16 depends from amended independent claim 68 and claim 50 depends from amended independent claim 73. Teppler does not overcome the deficiencies of Schneier and Den Boer relative to claims 68 and 73, described above. For at least these reasons, and further in view of their own features, claims 16 and 50 are patentable over the combination Schneier, Den Boer, and Teppler. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: July 17, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

558372_1 (2).DOC